Committee on
HOMELAND SECURITY
Chairman Michael McCaul

Opening Statement

May 21, 2014

Media Contact: Charlotte Sellmyer
(202) 226-8417

Statement of Subcommittee Chairman Patrick Meehan (R-PA)
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
Committee on Homeland Security

Assessing Persistent and Emerging Cyber Threats to the U.S. Homeland

Remarks as Prepared

I would like to thank everyone for attending this important hearing and Chairman King in particular for holding this as a joint hearing with the Subcommittee on Counterterrorism and Intelligence. This is the latest in a series of hearings the cybersecurity subcommittee has held examining the threat to our computer networks and what the US government is doing to mitigate and respond to that threat.

The threat of cyber attack is a real and growing menace to American security and prosperity. Over the past year alone, we have seen Iranian hackers disrupt the computer systems of Saudi energy company Aramco and attempt to take down the American financial sector. We have also seen criminals attack some of the icons of our retail sector, compromising the personal information of over 100 million customers. And just this week, the Department of Justice announced indictments against 5 Chinese military operatives for hacking into US companies to steal proprietary information.

Last month, I had the opportunity to travel to China with a number of my colleagues, including House Majority Leader Eric Cantor. We met with a number of China's most senior leaders and we specifically raised concerns about state-sponsored industrial espionage and the importance of protecting and respecting the intellectual property and trade secrets of American businesses. China has a responsibility to adhere to international law – a responsibility it has repeatedly failed to acknowledge.

The response we received from Chinese officials about these concerns was disciplined. The Chinese refused to admit that they condoned or supported their state-sponsored corporate espionage, and they refused to concede that American businesses were routinely targeted by Chinese hackers for intrusion.

In addition to state sponsored and criminal organizations, ideologically motivated actors, including terrorist groups and activists, use the internet to attack us and to finance their illicit activities. As the

2014 report by cybersecurity firm Mandiant states, "threat actors are not only interested in seizing the corporate crown jewels but are also looking for ways to publicize their views, cause physical destruction and influence global decision makers."

Defending against and responding to these attacks have a real cost and that cost is primarily borne by the American private sector. Companies spend hundreds of millions of dollars per year defending their networks. At a hearing we held last month, a Philadelphia area community bank testified that they spend a million dollars a year on cybersecurity efforts – and they could spend much more. Attacks that cause business disruptions cost companies an average of nearly $300,000 each to mitigate the damage. Companies who have lost untold amounts of intellectual property have found themselves at a competitive disadvantage with their global competitors. Identity theft alone costs US banks, retailers and consumers roughly $780 million per year.

All of these losses directly contribute to job losses, missed business opportunities and American companies at a competitive disadvantage on the world stage.

The question then becomes, how do we respond to this threat? First, we must ensure that our federal agencies have defined roles and are coordinating with each other and the private sector to share threat information. We must also crack down on the perpetrators of these attacks by arresting malicious hackers and pressuring other countries to do the same. That is especially true in China and Eastern Europe, where these corporate spies and criminals hide. The indictments of Chinese military hackers and the arrest of over 100 hackers linked to the malicious software called Blackshades are a good start but there is much more work to do.

Importantly, we in Congress need to understand this threat- who these adversaries are, what they want, where they live and what they are capable of doing. I look forward to hearing such details from our witnesses in the closed portion of this hearing.

###